

3/7

302 301 300 303

**BigFix Enterprise Console** [cadet] MS03-043:buffer:Buffer Overrunn Messenger Service Could Allow...

File Edit View Tools Window Help

Relevant Fixlet Message (58)

- By Name
- By Source Severity
  - <N/A> (2)
  - <Unspecified> (26)
  - Low (5)
  - Moderate (3)
  - Important (9)
  - Critical (19)

Name	Source Severity	Affected CO....
MS03-040: Cumulative	Critical	353
UPDATE: Windows XP Service Pack...	Critical	577
MS03-039: Buffer Overrun In RPLS...	Critical	129
MS03-043: Buffer Overrun In Mess...	Critical	157
MS03-043: Buffer Overrun In Mess...	Critical	
MS03-042: Buffer Overrun In Wind...	Critical	
MS03-030: Unchecked Buffer in Di...	Critical	
MS03-041: Vulnerability in Authen...	Critical	

Fixlet: Messages Computers Actions Console Operators

**Fixlet: MS03-043: Buffer Overrun in Messenger Service Could Allow Code Ex..** 1 Relevant Computers  
Severity: Critical 0 Open Actions

Description Relevant Computers Action History

**MS03-043: Buffer Overrun in Messenger Service Could Allow Code Execution - Windows 2000**

Microsoft has released a patch eliminating a "buffer overflow" vulnerability in Messenger Service. If properly exploited, a malicious user can cause arbitrary code to be executed with "Local System" privileges, or cause the Messenger Service to fail, after applying this patch, executed computers will no longer be susceptible to this vulnerability.

File Size: 312 KB

Click here to initiate the deployment process

Ready Connected to database "bfenterprise" a

310 305 304

FIG. 3

**BigFix Enterprise Console** [cadet] MS03-043:buffer:Buffer Overrunn Messenger Service Could Allow...

File Edit View Tools Window Help

By Source Severity

- <Unspecified> (26)
- Low (5)
- Moderate (1)
- Important (4)
- Critical (22)

Name	Affect...	Category	Size
MS03-043: Buffer Overrun In Messenger Servi...	129	Security Hotfix	En
MS03-043: Buffer Overrun In Messenger Servi...	18	Security Hotfix	En
MS03-042: Buffer Overflow in Windows Troub...	175	Security Hotfix	En
MS03-041: Vulnerability in Authenticode Verific...	170	Security Hotfix	En
MS03-041: Vulnerability in Authenticode Verific...	7	Security Hotfix	En
MS03-043: Buffer Overrun In messenger Servi...	1	Security Hotfix	En

Fixlet: Messages Computers Actions Console Operators

FIG. 4

4/7

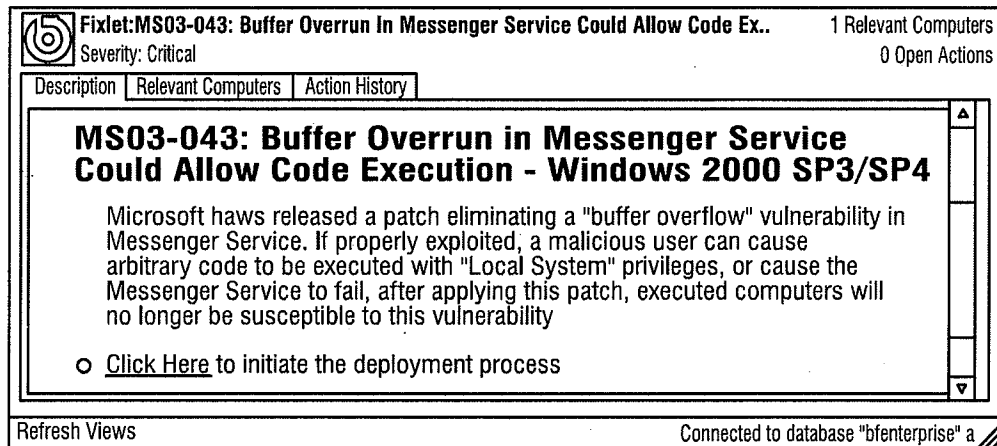


FIG. 5

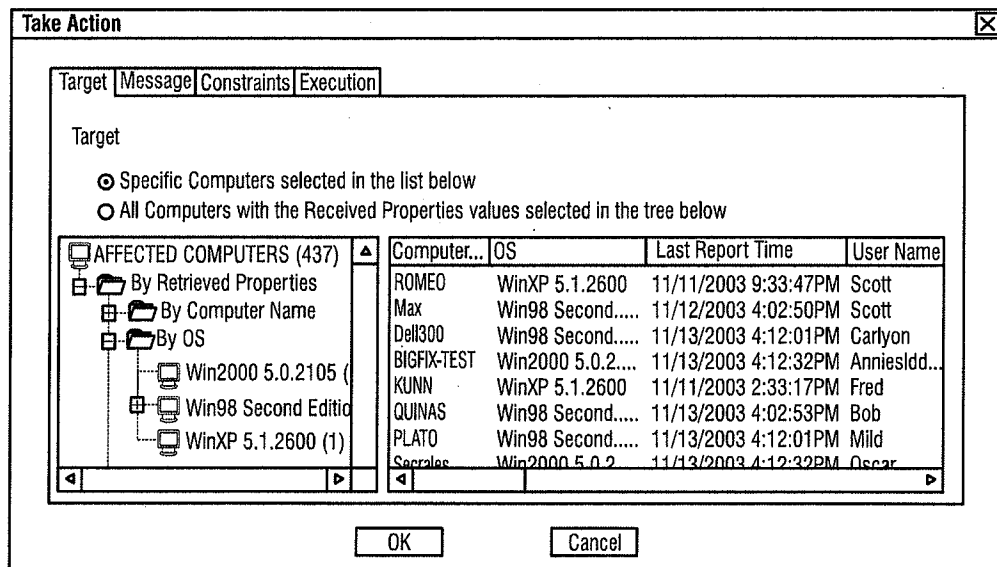


FIG. 6

5/7






 <b>Action: Assign Management Rights For Dennis</b>				4 Reported Computers		
Issued 10/19/2003 6:35:49 PM by John				4 Computers Fixed		
Repaired Computers	Target	Message	Constraints	Execution	Action Script	Relavance
<div><div><div><div><div></div><div>By Retrieved Properties</div></div><div><div></div><div>By Status</div></div><div><div></div><div>By Computer Name</div></div><div><div></div><div>By Local</div></div></div><div><div><div>▲</div></div></div></div></div>			<div><div>Status</div><div>Mixed</div><div>May</div></div>	<div><div>▲</div></div> <div>Computer Name</div> <div>ROMEO</div>		<div>Last Repd</div> <div>11/11/20</div>

FIG. 7

**BigFix Enterprise Console-[Computer "ROMEO"]**

All Actions (240)
 

By ID
 

By State
 

Explored (9)
 

Open(11)
 

By Name
 

By Link ID
 

By Site

ID	State	Name
69	Open	Restart Needed
68	Open	M
66	Open	M
65	Open	M
64	Open	C
62	Open	A
58	Open	C
50	Open	C

Open
 Copy
 Select All
 Show Action Info...
 Stop Action
 Restart Action

Internet Setting
 Candace

Fixlet: Messages
 Computers
 Actions
 Console Operators

FIG. 8






 Computer: DELL300 300 Mhz Pentium II Running Win98 Second Edition.67766448		27 Relevant Fixlet Messages 3 Open Actions																			
Relevant Fixlet Messages		Action History	Fixlet Message History	Retrieved Properties	Computer Settings	Management Rights															
 Relevant Fixlet Message  By Name  By Source Severity  <QUNAX> (1)		<table><thead><tr><th>Name</th><th>Source Sev...</th><th>Category</th></tr></thead><tbody><tr><td>MS02-044: Unsafe in Office Web Components</td><td>Critical</td><td>Enterprise</td></tr><tr><td>MS02-065: Buffer Overrun In Microsoft data a</td><td>Critical</td><td>Security Hotfi</td></tr><tr><td>MS03-042: Buffer Overflow</td><td></td><td></td></tr><tr><td>MS03-044</td><td></td><td></td></tr></tbody></table>					Name	Source Sev...	Category	MS02-044: Unsafe in Office Web Components	Critical	Enterprise	MS02-065: Buffer Overrun In Microsoft data a	Critical	Security Hotfi	MS03-042: Buffer Overflow			MS03-044		
Name	Source Sev...	Category																			
MS02-044: Unsafe in Office Web Components	Critical	Enterprise																			
MS02-065: Buffer Overrun In Microsoft data a	Critical	Security Hotfi																			
MS03-042: Buffer Overflow																					
MS03-044																					

FIG. 9

6/7

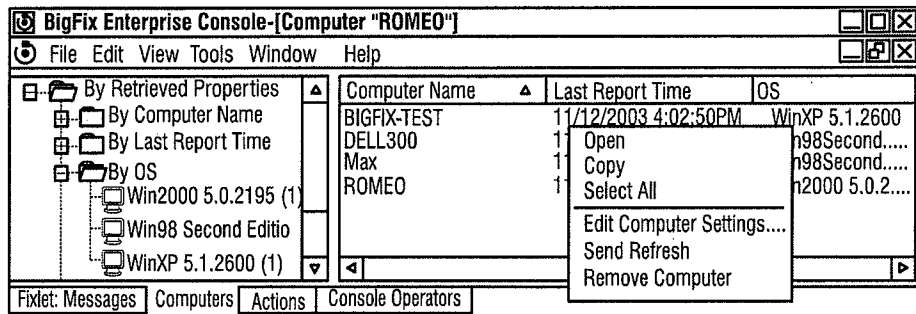


FIG. 10

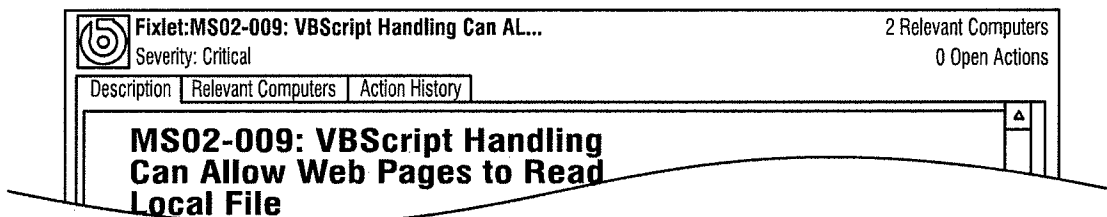


FIG. 11

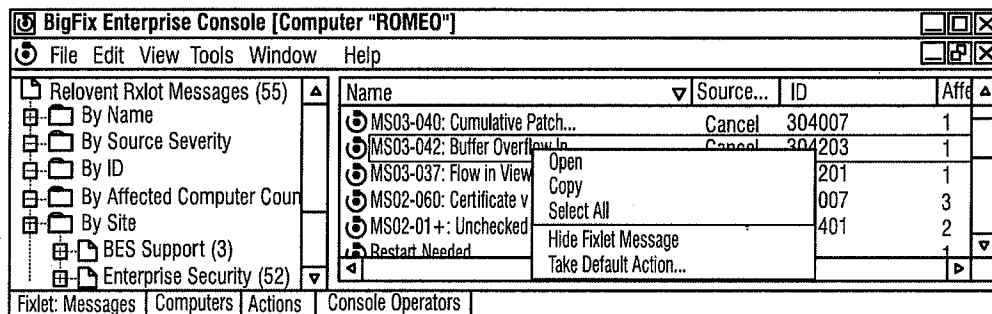


FIG. 12

7/7

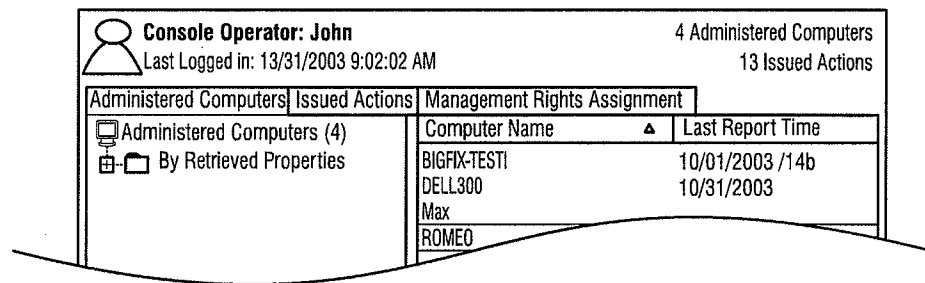


FIG. 13

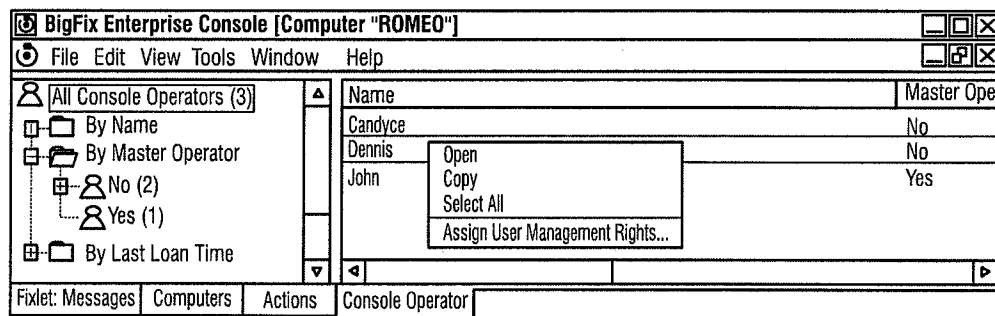


FIG. 14